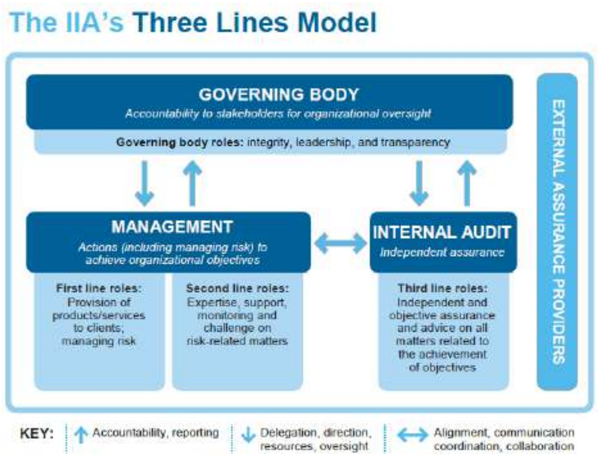
IIA Malaysia e-techline

August 2020 Issue 4/20

LATEST DEVELOPMENT FROM IIA GLOBAL

THE IIA'S THREE LINES MODEL: AN UPDATE OF THE THREE LINES OF DEFENSE


The IIA's Three Lines Model
GOVERNING BODY
Accountability to stakeholders for organizational oversight
Governing body roles: integrity, leadership, and transparency
MANAGEMENT
Actions (including managing risk) to achieve organizational objectives
First line roles: Provision of products/services to clients; managing risk
Second line roles: Expertise, support, monitoring and challenge on risk-related matters
INTERNAL AUDIT
Independent assurance
Third line roles: Independent and objective assurance and advice on all matters related to the achievement of objectives
EXTERNAL ASSURANCE PROVIDERS
KEY:
Accountability, reporting
Delegation, direction, resources, oversight
Alignment, communication coordination, collaboration

Key Roles in The Three Lines Model

A) The Governing Body

- Accepts accountability to stakeholders for oversight of the organisation.
- Engages with stakeholders to monitor their interests and communicate transparently on the achievement of objectives.
- Nurtures a culture promoting ethical behaviour and accountability**.**
- Establishes structures and processes for governance, including auxiliary committees as required.
- Delegates responsibility and provides resources to management for achieving the objectives of the organisation.
- Determines organisational appetite for risk and exercise oversight of risk management (including internal control).
- Maintains oversight of compliance with legal, regulatory and ethical expectations.
- Establishes and oversees an independent, objective and competent internal audit function.

B) Management

First Line Roles

- Leads and directs actions (including managing risk) and application of resources to achieve the objective of the organisation.
- Maintains a continuous dialogue with the governing body and reports on planned, actual and expected outcomes linked to the objectives of the organisations and risk.
- Establishes and maintains appropriate structures and processes for the management of operations and risk (including internal control).
- Ensure compliance with legal, regulatory and ethical expectations.

Second Line Roles

- Provide complementary expertise, support, monitoring and challenges related to the risk management, including:
  - ➢ The development, implementation and continuous improvement of risk management practices (including internal control) at a process, system and entity level.
  - ➢ The achievement of risk management objectives, such as compliance with laws, regulations and acceptable ethical behaviour; internal control; information and technology security; sustainability; and quality assurance.
- Provide analysis and reports on the adequacy and effectiveness of risk management (including internal control).

Internal Audit

- Maintains primary accountability to the governing body and independence from the responsibilities of management.
- Communicates independent and objective assurance and advice to management and the governing body on the adequacy and effectiveness of governance and risk

management (including internal control) to support the achievement of organisation objectives and to promote and facilitate continuous improvement.

- Reports impairment to independence and objectivity to the governing body and implements safeguards as required.

Relationship Among Core Roles

A) Between Management (Both First- and Second-Line Roles) and Internal Audit

There must be regular interaction between internal audit and management to ensure the work of the internal audit is relevant and aligned with the strategic and operational needs of the organisation, where internal audit contributes to the assurance and advice it delivers as a trusted advisor and strategic partner.

B) Between Internal Audit and the Governing Body

The governing body is responsible for oversight of internal audit, which requires: ensuring an internal audit function is established, including hiring and firing of Chief Audit Executive (CAE); serving as the primary reporting line for CAE; approving and resourcing the audit plan; receiving and considering reports from the CAE; and enabling free access by the CAE to the governing body, including private sessions without the presence of management.

What Internal Auditors should do?

Internal auditors should act in accordance with the roles highlighted in the above and also ensure its activities align with the objectives of the organisation.

Reference:

https://global.theiia.org/about/about-internal-auditing/Public%20Documents/Three-Lines-Model-Updated.pdf

INTERNAL AUDIT

WRITE EFFECTIVE AUDIT OBJECTIVES

Well-written objectives can define a successful internal audit

Audit objectives are the mission statement, or the reason, for the audit engagement. Once they have been established, everything done on the engagement either directly or indirectly support their achievement.

Audit objectives are one of the most important parts of the audit engagement, and they impact every aspect of it, including the:

- Audit scope, which determines how much evidence the auditors will review.
- Audit resources and how they will be deployed.
- Audit programme that will be developed to achieve the audit objectives.
- Audit results, which reflect the achievement of the audit objectives.

Well-written objectives are crucial to performing an effective audit. There are three basic principles that can help develop effective audit objectives. Each objective should:

1. Be simple and focused.
2. Seek to reach a conclusion.
3. Be traceable to the summary results.

IIA *Standards* Relative to Audit Objectives

Based on the International Standards for the Professional Practice of Internal Auditing, the chief audit executive (CAE), in consultation with management, must develop a risk-based plan to determine the areas of significant risk to the organisation.

Those areas are then prioritised to ensure that audit resources are deployed accordingly. A preliminary assessment, with input from management, is conducted for each audit. Using the preliminary assessment results, the CAE then develops the audit performed. objectives based on the selected risks, the available audit personnel, and the allotted time for the engagement.

Keep Objectives Simple and Focused

Each audit objective should be straightforward and not overly broad. It should be easy to identify what is to be accomplished. Using a bulleted list makes the audit objectives obvious and easy to follow. There is the added advantage that each bullet point can serve as an objective for developing a step-by-step audit programme. Plus, the bullet points can be directly correlated to the summary results.

Seek to Reach a Conclusion

Audit objective statements will generally have the words "to determine" or similar phrases such as "to assess," "to review," or "to evaluate." Audit objectives are essentially "yes or no" questions that seek some type of determination. Each objective should determine either "yes," the controls worked, or "no," they did not work or only partially worked.

Make Objectives Traceable to the Conclusion

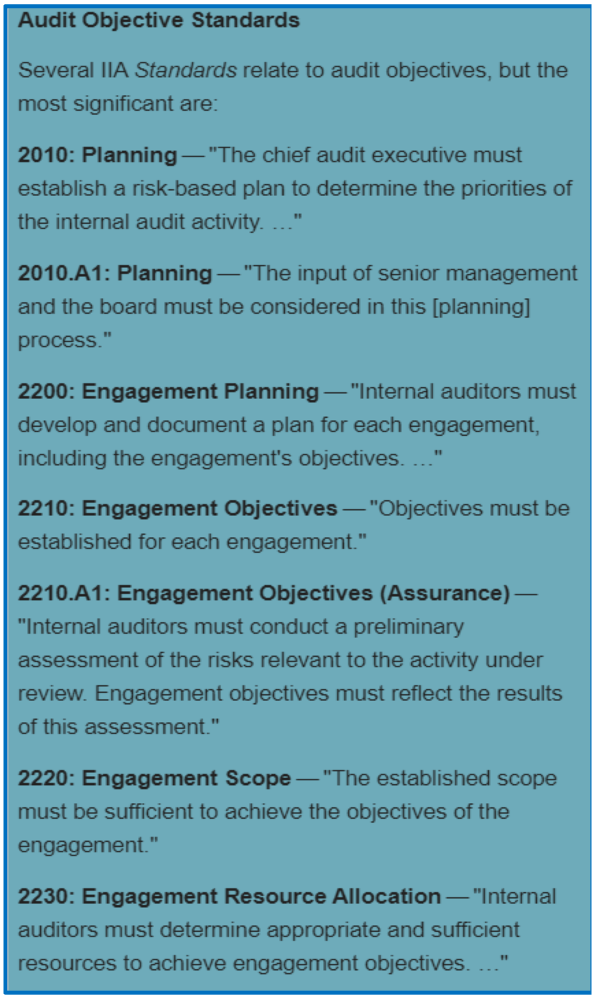
The summary of findings should be worded very similarly to, or mirror, the audit objectives. Summary conclusions should be in the same order and read almost exactly like the audit objectives were written, making them easily traceable back to the audit objectives.

What Internal Auditors should do?

Internal auditors should apply the three principles when developing audit objectives as it will make them more effective and useful. It will ensure that audit objectives will be effectively addressed, and audit resources can be more efficiently deployed.

Reference:

https://iaonline.theiia.org/2020/Pages/Write-Effective-Audit-Objectives.aspx



Audit Objective Standards

Several IIA *Standards* relate to audit objectives, but the most significant are:

2010: Planning — "The chief audit executive must establish a risk-based plan to determine the priorities of the internal audit activity. …"

2010.A1: Planning — "The input of senior management and the board must be considered in this [planning] process."

2200: Engagement Planning — "Internal auditors must develop and document a plan for each engagement, including the engagement's objectives. …"

2210: Engagement Objectives — "Objectives must be established for each engagement."

2210.A1: Engagement Objectives (Assurance) — "Internal auditors must conduct a preliminary assessment of the risks relevant to the activity under review. Engagement objectives must reflect the results of this assessment."

2220: Engagement Scope — "The established scope must be sufficient to achieve the objectives of the engagement."

2230: Engagement Resource Allocation — "Internal auditors must determine appropriate and sufficient resources to achieve engagement objectives. …"

GOVERNANCE

IS YOUR BOARD DIGITALLY SAVVY?

Boards and business leaders are aware of the digital revolution taking place across the globe and how digital leaders were able to navigate the choppy COVID-19 seas much more effectively than their less resilient peers. But what is being done to advance their organisations' digital capabilities? Specifically, does the board possess the digital savviness needed to support the CEO's efforts to continuously improve the company's business model, customer experience, decision-making processes, and operational efficiency and effectiveness?

Based on machine analysis of the various boards' digital capabilities, the research analysed data based on boards of U.S.-listed companies from surveys, interviews, company communications and the bios of 40,000 directors, extracting keywords indicating the ability to think and act digitally. According to the research, digitally savvy directors possess the following attributes:

- Firsthand knowledge of how technologies will impact the way companies can succeed in the next ten (10) years.
- An enterprise-level comprehension of innovative technologies, such as artificial intelligence, big data, the Internet of Things, scalable digital platforms and digital processes that enable new business models, enhance customer experiences and run operational efficiencies.
- An understanding of when to undertake new digital initiatives and the early indicators of when those initiatives are either grappling or succeeding.
- The instinctive ability to integrate digital thinking into the early stages of the strategy-setting process.

What Internal Auditors should do?

Internal auditors may share the following suggestions to the board to gain the next-generation knowledge:

- Board to look at the extent to which digital savviness is present in their oversight processes.
- Board to elevate their digital savviness through external experts' engagements as advisers, participating in self-directed digital training, and visiting "born digital" companies or companies have accomplished meaningful transformation activities.
- Board to ask the tough questions on what is really happening in the company and industry and to use technology as a strategic driver rather than a strategic enabler.
- Board must be capable of assessing chief information officer's and chief executive officer's capabilities and performances considering changing markets.

Reference:

https://www.protiviti.com/SG-en/insights/newsletter-bpro129-your-board-digitally-savvy

BURSA MALAYSIA AMENDS MAIN MARKET AND ACE MARKET LISTING REQUIREMENTS IN RELATION TO NEW ISSUES OF SECURITIES AND OTHER AREAS

On 13 August 2020, Bursa Malaysia Berhad amended the Main Market and ACE Market Listing Requirements, to enhance the disclosure requirements in connection with new issue of securities, as well as address gaps for greater shareholder protection and confidence.

Integrity and quality of the Board remain a key focus for the Exchange. Hence, the Exchange has also enhanced the definition of independent directors by extending the cooling-off period for specific persons to three years and subjecting a non-independent non-executive director to such revised cooling-off period. This is to strengthen the independence of a proposed director so that he is free from any business or other relationship which could interfere with the exercise of independent judgement of a director.

What Internal Auditors should do?

Internal auditors to stay aware of the latest development on the Bursa Guidelines.

Reference:

https://www.bursamalaysia.com/about_bursa/media_centre/bursa-malaysia-amends-main-market-and-ace-market-listing-requirements-in-relation-to-new-issues-of-securities-and-other-areas

GUIDELINES ON CONDUCT OF DIRECTORS OF LISTED ISSUERS AND THEIR SUBSIDIARIES

The Securities Commission Malaysia (SC) issued a new Guidelines on Conduct of Directors of Listed Issuers and heir Subsidiaries (Guidelines) to strengthen board governance and oversight in listed issuers and their subsidiaries.

The issuance of these guidelines is in line with the SC's Corporate Governance Strategic Priorities (2011-2020) which seeks to, among others, promote the proper discharge of directors' fiduciary duties among corporate Malaysia.

The Guidelines also set out guidance on duties and responsibilities of boards in company group structures and requirements for the establishment of a group-wide framework to enable, among others, oversight of group performance and the implementation of corporate governance policies.

"The new Guidelines take into account the evolving Malaysian corporate governance landscape, lessons learnt from the SC's regulatory work in enforcing corporate governance breaches and the need to ensure that Malaysia's framework remains relevant and effective. In discharging his fiduciary duties, a director owes the company duties of disclosure, honesty, candour and the duty to favour the company's interest over his own," said Datuk Syed Zaid Albar, Chairman of SC.

The introduction of these Guidelines is one of the measures approved by the Special Cabinet Committee on Anti-Corruption (JKKMAR) in 2019. The Guidelines comes into effect on 30 July 2020, with the exception of Chapter 5 on Group Governance which will come into effect on 1 January 2021.

The Guidelines are issued pursuant to section 158 and subsection 15(1)(q) of the Securities Commission Malaysia Act (SCMA).

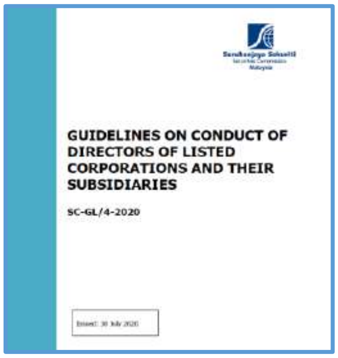
These Guidelines apply to directors of a listed corporation and directors of subsidiaries of a listed corporation whether incorporated in Malaysia or otherwise.

These Guidelines are in addition to and not in derogation of the requirements under the securities laws or other written law, guidelines issued by the SC or requirements imposed by the stock exchange.

What Internal Auditors should do?

The internal auditors need to be cognisant of the latest development of SC's guideline, where those guidelines can be a good input to the assurance and consulting engagement.

Reference:
https://www.sc.com.my/regulation/guidelines/conduct-of-directors



Suruhanjaya Sekuriti
Securities Commission
Malaysia

GUIDELINES ON CONDUCT OF DIRECTORS OF LISTED CORPORATIONS AND THEIR SUBSIDIARIES

SC-GL/4-2020

Issued: 30 July 2020

IIA Malaysia e-techline
August 2020 Issue 4/20

RISK MANAGEMENT

UNDERSTANDING CHANGES IN RESILIENCE RISKS FROM TECHNOLOGY ADVANCEMENTS

How resilient is our organisation? How do we track our organisation's change in resilience? Those are two of the most common questions posed by boards on the topic of resilience. The proper responses to these seemingly abstract questions require a firm understanding of the organisation's ability to recover important services and functions, as well as the ability to benchmark resilience, either on a comparative basis or using an organisational baseline.

Rather, to understand resilience, organisations must create a baseline recovery metric and map the change in recovery abilities (reduction in resilience risk) as policies and technologies are enhanced.

A common reaction to understanding recovery is to challenge recovery against established recovery time objectives (RTOs). This process can be prone to errors. When not mandated by regulation, RTOs are often used as abstract time periods developed through the qualitative assumptions of business heads who naturally have a bias to their businesses. RTO does not contemplate service or process-level recovery; meaning, the RTO of one system may not accurately reflect the time period required to begin a service or process after a resilience event.

Furthermore, regulators are moving towards requiring a cost or harm component against the time factor to understand what downtime means to an organisation and its stakeholders, and to define the degree of downtime that will cause irreparable harm to an important business service or process. This move does not align well with the concept of RTO.

Factor Analysis of Information Risk (FAIR), a method created to quantify unknown cybersecurity risks, can be used to measure resilience and derive significant organisational benefits and savings. Open source and industry-accepted, FAIR can be used to break down the cost of downtime to organisational stakeholders. All types of harm can be measured using this detailed process. Most importantly, the net aggregation of the output can be used to quantify an organisation's important services and processes, baseline resilience and impact tolerance, as proposed by the UK supervisory authorities.

Although FAIR was not developed for this purpose, this expanded use represents a logical extension of its intended use and the math that drives the standard. Clearly, to understand and quantify risks, the harm posed by an event must also be understood.

Using FAIR to Understand Change in Resilience Risk

Technology is a primary tool for enhancing organisational resilience. Software as a service (SaaS). Remote desktops. Public cloud providers. Internet of things (IoT). These technologies have had a significant impact on the ability of an organisation to withstand adverse events by, among other things, enabling the decoupling from a desktop, decreasing concentration risk, and providing enhancements in the storage and availability of data. The net effect of these technology advancements, on both the risk to an organisation and its ability to recover, cannot be overlooked.

The Capital Charge Effect

In the same way cost of downtime before and after implementation of new technology can be calculated using a method like FAIR, it is also possible to calculate the loss exposure reduction resulting from technology implementation – in other words, it is possible to quantify a potential reduction in a component of operational risk. This quantifiable decrease in operational risk can potentially help firms gauge how much capital to hold against operational risk as part of their Comprehensive Capital Analysis and Review (CCAR) and risk-weighted asset calculations.

Potential capital reductions may be realised by capturing improvements in operational risk management and loss mitigation during the capital measurement process. The current regulatory capital regime appropriately emphasises historical operational loss experience, as improvements in operational risk management are expected to reduce losses and lower capital charges over time. However, scenario analysis can reflect changes in operational risk on a timelier basis.

Stress Testing a Technology Project

There are numerous factors that go into selecting a technology project, however, quantifying resilience as a component of the project selection is not a common consideration. For most organisations, it is a challenge to contemplate the outcome of a project against desired resilience risk reduction. It is also a challenge to validate the success of the project against baseline estimates of the resilience risk reduction versus the anticipated reduction.

FAIR allows users to take numerous projects and stress test their anticipated outcomes. The anticipated effect of technology can be realised before and after the project is complete, allowing for a more comprehensive view of:

a) Project selection
b) Project Outcome
c) Return on investment

What Internal Auditors should do?

Having a process to keep your board well informed about the organisation's level of resilience and how changes to resilience are tracked is critical:

- The internal auditor should start with calculating the organisation's initial level of resilience using FAIR and reporting that information to the board. With this information, the board can effectively assess the recovery of the organisation or important business service or process and can understand the related potential downtime and cost assumptions.

- Then, when the board asks what the organisation is doing to enhance the resilience of the organisation, overlaying the reduction of resilience risk from planned projects will provide a simple but effective visual response to the query.

- Finally, updating resilience risk from completed projects will re-baseline the overall level of resilience, allowing the board to understand the exposure in time and dollars and any changes in exposure to the firm.

Reference:

https://www.protiviti.com/SG-en/insights/pov-technology-advancements-resilience-risks